BEST AVAILABLE IMAGES

Defective images within this document are accurate representations of the original documents submitted by the applicant.

Defects in the images may include (but are not limited to):

- BLACK BORDERS
- TEXT CUT OFF AT TOP, BOTTOM OR SIDES
- FADED TEXT
- ILLEGIBLE TEXT
- SKEWED/SLANTED IMAGES
- COLORED PHOTOS
- BLACK OR VERY BLACK AND WHITE DARK PHOTOS
- GRAY SCALE DOCUMENTS

IMAGES ARE BEST AVAILABLE COPY.

As rescanning documents *will not* correct images, please do not report the images to the Image Problem Mailbox.

BUNDESREPUBLIK DEUTSCHLAND

Prioritätsbescheinigung über die Einreichung einer Patentanmeldung

Aktenzeichen:	199 58 721.3
Anmeldetag:	6. Dezember 1999
Anmelder/Inhaber:	Francotyp-Postalia AG & Co, Birkenwerder/DE
Bezeichnung:	Frankierverfahren und -vorrichtung
IPC:	G 07 B 17/04

Die angehefteten Stücke sind eine richtige und genaue Wiedergabe der ursprünglichen Unterlagen dieser Patentanmeldung.

München, den 18. September 2000
Deutsches Patent- und Markenamt
Der Präsident
Im Auftrag

A 9161
03/00
EDV-L

Eisenführ, Speiser & Partner

Bremen
Patentanwälte
European Patent Attorneys
Dipl.-Ing. Günther Eisenführ
Dipl.-Ing. Dieter K. Speiser
Dr.-Ing. Werner W. Rabus
Dipl.-Ing. Jürgen Brügge
Dipl.-Ing. Jürgen Klinghardt
Dipl.-Ing. Klaus G. Göken
Jochen Ehlers
Dipl.-Ing. Mark Andres

Rechtsanwälte
Ulrich H. Sander
Sabine Richter

Martinistrasse 24
D-28195 Bremen
Tel. +49-(0)421-36 35 0
Fax +49-(0)421-337 8788 (G3)
Fax +49-(0)421-328 8631 (G4)
mail@eisenfuhr.com

Hamburg
Patentanwalt
European Patent Attorney
Dipl.-Phys. Frank Meier

Rechtsanwälte
Christian Spintig
Rainer Böhm

München
Patentanwälte
European Patent Attorneys
Dipl.-Wirtsch.-Ing. Rainer Fritsche
Lbm.-Chem. Gabriele Leißler-Gerstl
Patentanwalt
Dipl.-Chem. Dr. Peter Schuler

Berlin
Patentanwälte
European Patent Attorneys
Dipl.-Ing. Henning Christiansen
Dipl.-Ing. Joachim von Oppen
Dipl.-Ing. Jutta Kaden

Alicante
European Trademark Attorney
Dipl.-Ing. Jürgen Klinghardt

Bremen, den 3. Dezember 1999

Unser Zeichen: F 735 KGG/pls/ssi/wib

Anmelder/Inhaber: Francotyp-Postalia AG
Amtsaktenzeichen: Neuanmeldung

Francotyp-Postalia AG & Co., Triftweg 21 - 26, 16547 Birkenwerder

---

Frankierverfahren und -vorrichtung

Die Erfindung betrifft ein Verfahren zum maschinellen Frankieren von Postgut und zur Prüfung der Frankierung gemäß dem Oberbegriff des Anspruches 1 sowie ein Verfahren gemäß dem Oberbegriff des Anspruches 11. Die Erfindung betrifft außerdem ein System zur Durchführung eines solchen Verfahrens gemäß dem Oberbegriff des Anspruches 12 sowie eine Frankiermaschine zum maschinellen Frankieren von Postgut gemäß dem Oberbegriff des Anspruches 15.

Wie viele andere Unternehmen betreiben auch Postdienste in vielen Ländern der Erde zunehmend Handel auf elektronischem Wege, sogenannten Electronic Commerce (e-commerce). Traditionell benutzen größere Unternehmen Frankiermaschinen zur Frankierung ihrer Postgüter. Derartige Frankiermaschinen sind an registrierte Personen lizenziert und erfordern eine bestimmte Verbindung zu dem Postdienst, um Postgebühren für die Frankierung nachladen zu können. In einem solchen geschlossenen Frankiersystem werden mechanische Frankiermaschinen mittels physikalischer Jetons (tokens) nachgeladen, oder es bestehen bei elektronischen Frankiermaschinen Verbindungen zu dem Postdienst über eine spezielle Leitung oder die Telefonleitung, um Postgebühren von einem dortigen Gebührenrechner herunterzuladen. Derartige Frankiermaschinen werden nur an registrierte Kunden verkauft oder geleast, und eine Inspektion durch die Postdienste ist in regelmäßigen Abständen erforderlich.

Da inzwischen auch kleinere Unternehmen und Büros ausreichend Rechenleistung auf Computern und Druckern zur Verfügung haben und ein Internetanschluss einfach und günstig zur Verfügung steht, werden vermehrt Frankiersysteme benutzt, mit denen Postgebühren über offene Netzwerke wie das Internet von dem Postdienst heruntergeladen werden können und die keine besondere Hardware mit regelmäßigem Inspektionsbedarf erfordern. Bei solchen sogenannten offenen Frankiersystemen kann ein herkömmlicher PC zum Herunterladen von Postgebühren und ein Standarddrucker zum Drucken eines Gebührenstempels auf einen Briefumschlag oder ein Etikett benutzt werden.

Der US-Postdienst hat eine Systemarchitektur für offene und geschlossene Frankiersysteme spezifiziert. Ein solches System ist beispielsweise aus der US 5,825,893 bekannt. Jeder Benutzer verfügt dabei über ein physikalisches möglichst aufbruchsicheres Sicherheitsgerät, auf dem alle für die Frankierung vorgesehenen Postgebühren des Benutzers gespeichert sind. Dieses Sicherheitsgerät (PSD = Postal Security Device) kann innerhalb oder außerhalb der Frankiermaschine oder des Computers angeordnet sein. In dem Sicherheitsgerät ist im wesentlichen ein Gebührenzähler und ein benutzer-individuelles Verschlüsselungsmodul angeordnet, mit dem der Gebührenstempel und ein weiterer maschinenlesbarer Datenstempel, sogenannte "Indizia", erzeugt werden. Zum Frankieren eines Stückes Postgut wird von dem Sicherheitsgerät ein solches Indizium aus der zu frankierenden Postgebühr, einem Identifizierungscode des Sicherheitsgerätes, der Absenderadresse, dem aktuellen Gebührenzählerstand und gegebenenfalls weiteren Daten mittels eines Unterschriftenschlüssels erzeugt. Dieses Indizium wird dann in einen zweidimensionalen Barcode codiert und auf das Postgut aufgedruckt, so dass es einfach und zuverlässig von einer Prüfeinrichtung des Postdienstes gescannt und überprüft werden kann. Der interne Postgebührenzähler der Frankiermaschine wird anschließend um den verwendeten Postgebührenbetrag verringert.

Da die Benutzer von offenen Frankiersystemen nicht registriert sind und die verwendete Hardware keinen regelmäßigen Inspektionen durch den Postdienst unterliegt, müssen derartige Frankiersysteme in stärkerem Maße gegen Betrug geschützt werden als geschlossene Frankiersysteme. Sie müssen jedoch auch deutlich billiger sein, um in den Massenmarkt vordringen zu können. Der Erfindung liegt deshalb die Aufgabe zugrunde, ein Frankierverfahren, ein Frankiersystem und eine Frankiermaschine zu schaffen, welche eine hohe Sicherheit gegen Betrug bei gleichzeitig niedrigen Kosten aufweisen.

Diese Aufgaben werden durch die Verfahren gemäß Anspruch 1 und Anspruch 11, durch das System gemäß Anspruch 12 beziehungsweise die Frankiermaschine gemäß Anspruch 15 gelöst.

Der Erfindung liegt dabei der Gedanke zugrunde, dass ein Betrug durch mehrfache Verwendung von Postgebühren und/oder mehrfache Verwendung von Datenstempeln dadurch verhindert werden kann, dass der bei der Frankierung auf das Postgut aufgebrachte maschinenlesbare Datenstempel derart codiert und/oder ausgestaltet wird, dass er sich eindeutig von anderen benutzten Datenstempeln unterscheiden lässt. Hierbei enthält der Datenstempel den Abdruck und/oder Wert einer für die vorliegende Frankierung individualisierten elektronischen Münze. Während übliches Geld, beispielsweise Münzen und Scheine zwar gängige Zahlungsmittel sind, lässt sich ihnen selbst aber nicht der Zahlungszweck ansehen. Bei der vorliegenden Erfindung wird jedoch mit der Frankierung ein für die vorliegende Frankierung individualisiertes Geld – nachfolgend elektronische Münze genannt – generiert, wobei diese elektronische Münze nicht nur einen Geldwert – wie beispielsweise Portowert – enthält, sondern darüberhinaus auch die Frankierung individualisierte Daten, so dass eine doppelte Generierung einer elektronischer Münze ausgeschlossen ist. Die elektronische Münze wird auf dem Postgut durch einen Datenstempel repräsentiert, welcher neben der Portowertangabe noch weitere die elektronische Münze identifizierende Angaben enthält, die maschinenlesbar sind. Dadurch kann der Postdienst mittels einer Prüfeinrichtung überprüfen, ob ein Datenstempel bereits benutzt worden ist und von einem Betrüger beispielsweise ausgeschnitten und auf einen neuen Brief aufgeklebt worden ist. Auch die mehrfache Verwendung von Postgebühren, die in derartigen Frankiersystemen in elektronischer Form gespeichert und abgerechnet werden, kann dadurch detektiert werden, da anhand des Datenstempels erkennbar ist, ob er mittels einer bereits verbrauchten Postgebühr erzeugt worden ist. Sofern in dem Datenstempel der Ersteller des Datenstempels (in nicht manipulierbarer (verschlüsselter) Form) enthalten ist, kann in diesem Fall auf den Betrüger geschlossen werden. In beiden Fällen können die mit derartigen betrügerischen Mitteln frankierten Postgüter von der Weiterbeförderung ausgeschlossen werden.

Gegenüber bekannten Lösungen weist die erfindungsgemäße Lösung die Vorteile auf, dass hierbei keine zusätzliche Hardware wie ein beschriebenes Sicherheitsgerät zum Speichern und Abrechnen der Postgebühren und zum Speichern eines benutzer-

individuellen Unterschriftenschlüssels erforderlich ist und als reine Softwarelösung auf einem konventionellen Computer realisiert werden kann. Weiter ist es nicht zwingend erforderlich, dass in dem Datenstempel Daten über den Benutzer enthalten sind, so dass aus dem Datenstempel nicht auf den Benutzer geschlossen werden kann, wodurch die Anonymität des Benutzers gewahrt wird. Es ist auch nicht erforderlich, dass neben dem Benutzer und dem Postdienst eine dritte Person als Überwachungsinstanz wie bei manchen bekannten Lösungen den Frankiervorgang und die Abrechnung der Postgebühren online überwacht, sondern eine Frankierung kann jederzeit und ohne Einschaltung einer solchen Überwachungsinstanz erfolgen. Insgesamt wird mit der erfindungsgemäßen Lösung ein ähnlich hoher Sicherheitsstandard wie bei kryptografisch sicheren elektronischen Zahlungssystemen erreicht.

In einer Ausgestaltung des erfindungsgemäßen Verfahrens ist vorgesehen, dass die Prüfung durch Vergleiche des zu prüfenden Datenstempels mit in einer Datenbank gespeicherten benutzten Datenstempeln erfolgt. Die Vergleichsprüfung der zu prüfenden Datenstempel ist gleichbedeutend mit der Vergleichsprüfung von generierten elektronischen Münzen. Da für jedes Stück Postgut ein individueller Datenstempel, also auch eine individuelle, das Poststück individualisierende elektronische Münze erzeugt wird, stellt dies eine einfache Realisierung der Prüfung dar, wobei die Datenbank in einer geeigneten Speichereinrichtung in der Prüfeinrichtung abgelegt ist. Da in der Praxis die Datenbank jedoch keinen unbegrenzten Speicherplatz aufweist, ist die Ausgestaltung gemäß Anspruch 3 sehr vorteilhaft. Jeder Datenstempel weist dabei ein Verfallsdatum auf, d.h. ein vom Tag der Erstellung des Datenstempels in der Zukunft liegendes Datum, bis zu dem der Datenstempel (bzw. die elektronische Münze) gültig ist und bis zu dem beispielsweise auch das Poststück befördert wird. Dieser Zeitraum kann zum Beispiel standardmäßig 14 Tage für alle Benutzer und alle Datenstempel (bzw. elektronische Münzen) betragen. Dies bedeutet, dass eine elektronische Münze, deren Verfallsdatum bei der Überprüfung bereits abgelaufen ist, in einer ersten Stufe der Überprüfung ausgesondert werden kann und dass in der Datenbank nur diejenigen benutzten elektronischen Münzen gespeichert bleiben müssen, die in diesem vom Tag der Überprüfung gerechneten zurückliegenden Zeitraum, im Beispiel also in den letzten 14 Tagen, überprüft worden sind. Dadurch kann beispielsweise jeden Tag wieder Speicherplatz in der Datenbank zur Verfügung gestellt werden durch Löschen der Datenstempel bzw. elektronischen Münzen mit den ältesten Überprüfungsdaten.

Die Weiterbildung der Erfindung gemäß Anspruch 4 stellt eine Möglichkeit dar, durch die eine Prüfung auf mehrfache Verwendung von Postgebühren erfolgen kann. Die Weiterbildungen gemäß den Ansprüchen 5 und 6 dienen im wesentlichen dem Bedienungskomfort, indem der Benutzer die zu frankierende Postgebühr aus einzelnen Postgebühreneinheiten zusammensetzen oder eine größere Postgebühreneinheit in kleine Untereinheiten unterteilen kann.

Um einerseits die genannte Prüfung von Postgebühren auf mehrfache Verwendung zu ermöglichen und andererseits zu verhindern, dass Betrüger sich selbst Postgebühreneinheiten erstellen, ohne dafür zu bezahlen, ist gemäß der Weiterbildung nach Anspruch 7 eine individuelle Codierung der Postgebühreneinheiten durch den Postdienst mit einem geheimen Schlüssel vorgesehen. Diese Codierung, die für jede Postgebühreneinheit unterschiedlich ausfällt, findet sich auch in dem auf das Postgut aufgebrachten Datenstempel wieder, an dem sich somit eine mehrfache Verwendung von Postgebühreneinheiten erkennen lässt.

Gemäß einer bevorzugten Weiterbildung der Erfindung sind in dem Datenstempel dessen Erstelldatum und Erstellzeit, die frankierte Postgebühr und der Adressat des Postguts in nicht manipulierbarer Form enthalten. Es kann jedoch auch vorgesehen sein, dass andere und/oder weitere Daten wie beispielsweise der Absender, dessen Anschrift oder ein Verfallsdatum für die Postgebühr enthalten sind.

Aus Kapazitätsgründen kann es vorgesehen sein, dass nicht alle Frankierungen und Datenstempel überprüft werden. So kann es vorgesehen sein, dass die Überprüfung nur stichprobenhaft durchgeführt wird, dass nicht alle überprüften Datenstempel in der Datenbank gespeichert werden oder dass ein zu überprüfender Datenstempel aus Zeitgründen nur mit einem Teil der in der Datenbank gespeicherten Datenstempel verglichen wird. Um dennoch zu verhindern, dass Gebührenstempel und Datenstempel von einem beförderten Postgut abgelöst oder abgeschnitten oder mittels eines Kopierers abkopiert und auf ein zu frankierendes Postgut einfach aufgeklebt oder aufkopiert werden, können bei der Weiterbildung gemäß Anspruch 9 weitere Postgutdaten in den Datenstempel mit aufgenommen werden. Diese Postgutdaten dienen quasi als individueller Fingerabruck des zu frankierenden Postgutes und fallen somit für jedes Postgut anders aus. Als Postgutdaten können beispielsweise die Oberflächenstruktur (Oberflächenfaserstruktur, Rauhigkeit der Oberfläche) des Verpackungsmaterials oder des Briefumschlages oder eine andere messbare, das einzelne Stück Postgut individualisierende Eigenschaft, wie z.B. das exakte Gewicht

verwendet werden, die vom Benutzer entweder eingegeben oder mittels einer in die Frankiermaschine integrierten Messeinrichtung automatisch bei der Frankierung gemessen werden.

Ausgehend von dieser Überlegung kann gemäß Anspruch 10 weiter vorgesehen sein, dass diese Postgutdaten künstlich in Form von auf einem Etikett befindlichen Etikettdaten dem Postgut hinzugefügt werden. Ein solches Etikett kann beispielsweise ein Hologramm oder einen Barcode tragen, dessen Daten als Postgutdaten mit in den Datenstempel integriert werden. Durch die Maßnahmen gemäß den Ansprüchen 9 und 10 wird erreicht, dass ein Datenstempel auch zu dem damit frankierten Postgut gehören muss und nicht für ein anderes Postgut verwendet werden kann, welches andere Postgutdaten aufweist. Dies kann bei der Überprüfung des Datenstempels festgestellt werden, sofern die Prüfeinrichtung in geeigneter Weise zur Messung der Postgutdaten des zu prüfenden Postgutes ausgestaltet ist und diese gemessenen Postdaten dann mit den in dem Datenstempel enthaltenen Postgutdaten verglichen werden.

Das Verfahren gemäß Anspruch 11, das auf einer einzelnen Frankiermaschine ausgeführt werden kann, kann in Ausgestaltungen wie das oben beschriebene Verfahren weitergebildet sein. Auch das in den Ansprüchen 12 bis 14 angegebene System zur Durchführung des Verfahrens nach Anspruch 1 sowie die in den Ansprüchen 15 und 16 angegebene Frankiermaschine können in entsprechender Weise ausgestaltet sein.

Die Erfindung wird nachfolgend anhand der Zeichnungen beispielhaft näher erläutert. Es zeigen:

Figur 1	das Blockschaltbild eines erfindungsgemäßen Frankiersystems;
Figur 2	ein nach dem erfindungsgemäßen Verfahren frankiertes Postgut;
Figur 3	das zum Eröffnen eines Postgebührenkontos abgearbeitete Protokoll;
Figur 4	das zum Herunterladen einer Postgebühreneinheit abgearbeitete Protokoll;
Figur 5	das zur Erzeugung eines Datenstempels abgearbeitete Protokoll;
Figur 6	das zur Detektion der doppelten Verwendung einer Postgebühreneinheit abgearbeitete Protokoll.

Figur 7 zeigt einen beispielhaften Abdruck (eines Datenstempels bzw. einer elektronischen Münze) mit einer Datenmatrix von 40 x 40 Elementen

Das in Figur 1 gezeigte Frankier- und Postbeförderungssystem weist einen Postdienst 1, eine Frankiermaschine 2 und einen Postbeförderungsdienst 3 auf. Der Postdienst 1 weist im wesentlichen eine Postgebühreneinrichtung 11 zum Ausgeben und Abrechnen von Postgebühreneinheiten und eine Prüfeinrichtung 13 zur Prüfung und Entwertung von Frankierungen auf. Die Postgebühreneinrichtung 11, die nicht zwingend in einem Postamt angeordnet sein muss, sondern beispielsweise auch durch eine dritte Partei oder im Internet lokalisiert sein kann, stellt Postgebühreneinheiten zur Frankierung von Postgütern zur Verfügung, die von dem Benutzer einer Frankiermaschine jederzeit erworben oder elektronisch heruntergeladen werden können. Mittels einer Einrichtung 12 werden die Postgebühreneinheiten (d.h. elektronische Münzen) bei der Ausgabe erzeugt, die Abrechnung und Buchführung erfolgt mittels einer Buchführungseinrichtung 15.

Die Frankiermaschine 2 weist eine Zentraleinheit 21 und eine Druckeinheit 22 auf, welche in einem offenen Frankiersystem durch einen Standard-PC und einen Standard-Drucker realisiert sein können. Die Zentraleinheit 21 umfasst ein Gebührenmodul 23, das die Postgebühreneinheiten von dem Postdienst 1 herunterlädt, speichert und bei einer Frankierung intern abrechnet. Die Speicherung von Postgebühren kann dabei beispielsweise auf der Festplatte des PCs, auf einer Chip-Karte oder auf einem anderen Speichermedium erfolgen. Die Abrechnung von Postgebühren mit dem Postdienst erfolgt in der Regel beim Herunterladen von Postgebühren vom Postdienst 1, während die interne Abrechnung beim Ausdrucken einer Frankierung erfolgt. Die Abrechnung mit dem Postdienst kann dabei mittels eines eigens eingerichteten Abrechnungskontos, mittels Kreditkarte, durch elektronische Zahlung oder durch Barzahlung erfolgen. Um Daten für die Erzeugung des Datenstempels bei der Frankierung eines Postguts gegen Manipulation zu schützen, ist weiter ein kryptographisches Modul 24 vorgesehen. Zur Drucksteuerung ist schließlich ein Drucksteuermodul 25 vorgesehen, welches die Druckeinrichtung 22 steuert. Der Gebührenstempel und der Datenstempel können entweder direkt auf das Postgut oder ein auf das Postgut aufzuklebendes Etikett gedruckt werden. Das frankierte Postgut wird anschließend von einem Postbeförderungsdienst 3 befördert, wobei es entweder dort oder in dem Postdienst 1, zum Beispiel in einer Postsammelstelle, eine Prüfeinrichtung 13 durchläuft, wo die Frankierung geprüft und entwertet wird. Dazu weist die

Prüfeinrichtung 13 eine Speichereinrichtung 14 auf, in der insbesondere benutzte Datenstempel gespeichert sind, mit denen ein zu prüfender Datenstempel verglichen wird. Zwischen der Postgebühreneinrichtung 11 und der Prüfeinrichtung 13 kann auch eine Verbindung bestehen, um beispielsweise über benutzte und entwertete Postgebühreneinheiten Buch zu führen und sicherzustellen, dass die Prüfeinrichtung 13 die Codierung von Postgebühreneinheiten kennt, die sich in regelmäßigen Zeitabständen ändern kann.

Die Frankierung, die im vorliegenden Fall wenigstens einen Gebührenstempel und einen Datenstempel aufweist und im allgemeinen als "Indizium" bezeichnet wird, sollte wenigstens die frankierte Postgebühr und eine elektronische Unterschrift zur Autorisierung dieser Postgebühr aufweisen. Zusätzlich können weitere Daten vorgesehen sein um spezielle Funktionen des Postbeförderungssystems zu unterstützen. Beispielsweise kann in maschinenlesbarer Form die Zustelladresse enthalten sein um automatische Postsortierung zu ermöglichen. Aus Anonymitätsgründen kann die Identität des Absenders dabei auch weggelassen werden. Der maschinenlesbare Teil der Frankierung kann beispielsweise in Form eines zweidimensionalen Barcodes aufgedruckt sein. Wenn sich eine Frankierung als gültig und ausreichend herausstellt, wird das Postgut an den entsprechenden Empfänger geliefert.

Ein solches Frankier- und Postbeförderungssystem muss soweit wie möglich gegen Betrug geschützt sein; Gebührenkonten von Benutzern müssen gesichert sein gegen unberechtigten Zugriff; Datenschutz und Anonymität muss in gewissen Grenzen gewahrt sein, und andere Sicherheitsanforderungen müssen berücksichtigt werden, die im folgenden näher erläutert werden sollen.

a) Zu jedem Zeitpunkt soll das Postbeförderungssystem nur soviel Post befördern, wie durch entrichtete Gebühren abgedeckt ist. Als Unterkriterium soll die doppelte Verwendung von Postgebühren verhindert werden: Nachdem ein Benutzer Postgebühren im Wert von x heruntergeladen hat, soll er maximal Gebührenstempel ausdrucken können, deren Gesamtwert den Wert x nicht überschreitet. In offenen Frankiersystemen ist in der Regel die Empfängeradresse und eine Zeitmarkierung bereits in dem Datenstempel enthalten, so dass dadurch eine erneute Benutzung einer bereits benutzten Frankierung auch ohne weitere kryptografische Schutzmaßnahmen weitgehend ausgeschlossen ist. In geschlossenen Frankiersystemen, in denen der Frankiervorgang getrennt ist von dem Adressierungsvorgang, so dass die Empfängeradresse in der Regel nicht in dem

Datenstempel enthalten ist, können Kopien von Frankierungen jedoch dadurch detektiert werden, dass wie bei dem erfindungsgemäßen System Frankierungen, d.h. der Datenstempel einer Frankierung, mit bereits benutzten und in einer Datenbank gespeicherten Frankierungen verglichen und überprüft wird. Wenn dabei ein Datenstempel ein zweites Mal detektiert wird, so kann das damit frankierte Postgut entweder mit einem Strafporto belegt an den Absender zurückgesandt oder von der Postbeförderung ausgeschlossen werden. Als weitere Schutzmaßnahme gegen Kopien von Frankierungen kann die Verwendung von roter fluoreszierender Tinte für den Gebühren- und/oder Datenstempel vorgesehen sein, die nur schwer mit herkömmlichen Kopierern zu reproduzieren ist. Um einen Benutzer zu identifizieren, der eine Postgebühreneinheit mehrfach zur Frankierung in illegaler Weise benutzt, kann beispielsweise weiter vorgesehen sein, dass der Datenstempel Daten über diesen Benutzer in in nicht manipulierbarer Form enthält, zum Beispiel die Nummer seines Postgebührenkontos oder einen speziellen Benutzercode.

b) Sofern es möglich ist, anhand des Datenstempels einen Benutzer zu ermitteln, der illegalerweise Frankierungen und/oder Postgebühreneinheiten mehrfach verwendet, müssen Schutzmaßnahmen getroffen werden, dass nicht irrtümlicherweise ein sich korrekt verhaltender Benutzer eines solchen Fehlverhaltens bezichtigt werden kann.

c) Frankierungen sollten nicht erkennen lassen, ob sie vom selben Benutzer her stammen, außer wenn der Absender/Benutzer dies wünscht. Außerdem sollte sich aus der Frankierung auch nicht die Absenderidentität ergeben, um die anonyme Absendung von Postgütern zu ermöglichen. So soll auch eine Verknüpfung von Datenstempeln durch Vergleich der Benutzer verhindert werden.

Zusätzlich zu den beschriebenen Sicherheitsanforderungen sollte ein Frankiersystem auch ausreichend Bedienungskomfort anbieten. Nach dem Herunterladen von Postgebühren im Werte von x, sollte der Benutzer die Möglichkeit haben, jeden beliebigen Gebührenwert (maximal x) zu erzeugen. Außerdem sollten der Vorgang des Erwerbs von Postgebühreneinheiten und der Erzeugung von Frankierungen voneinander unabhängig sein, so dass nicht wie bei bekannten Systemen zur Erzeugung einer Frankierung erst eine Online-Verbindung zu einer Postgebühreneinrichtung hergestellt werden muss, um eine Postgebühr herunterzuladen, welche unmittelbar in eine Frankierung umgewandelt wird. Die Frankierung sollte also auch offline und ohne Ein-

schaltung einer dritten, die Frankierung und die Abrechnung der Postgebühr überwachenden Einrichtung möglich sein.

Mit dem erfindungsgemäßen Verfahren und dem gezeigten erfindungsgemäßen System können die beschriebenen Sicherheitserfordernisse und der beschriebene Bedienkomfort erreicht werden. Durch die individuelle Gestaltung der Datenstempel derart, dass beispielsweise jeden Tag ein anderer Typ von Datenstempeln erforderlich ist für jeden Adressaten, kann die doppelte Verwendung von Frankierungen weitgehend ausgeschlossen werden. Ein Betrüger, der ein Postgut an einen bestimmten Empfänger gesandt hat, könnte die dazu benutzte Frankierung ein zweites Mal nur für eine zweite Sendung am selben Tage benutzen. Da weiter vorgesehen ist, dass in der Prüfeinrichtung die Datenstempel mit den in der Datenbank gespeicherten bereits benutzten und in Datenstempeln verglichen werden, können zum zweiten Mal benutzte Frankierungen mit hoher Sicherheit detektiert werden. Wenn die Erzeugung des Datenstempels derart ausgestaltet ist, dass Informationen über die Identität des Benutzers enthalten sind, kann dieser im Falle eines Betrugs auch ermittelt werden. Da in dem Datenstempel auch ein Code enthalten ist, aus dem sich auf die verwendete Postgebühreneinheiten zur Erzeugung der Frankierung schließen lässt, kann bei dieser Überprüfung auch festgestellt werden, ob die entsprechende Postgebühreneinheiten bereits früher zur Erzeugung einer Frankierung benutzt und deshalb verbraucht ist. Da die Postgebühreneinheiten auch jederzeit und unabhängig vom Zeitpunkt einer vorzunehmenden Frankierung erworben und heruntergeladen werden können und sich sowohl in kleinere Untereinheiten unterteilen als auch zu größeren Einheiten kombinieren lassen, ist auch der geforderte Bedienungskomfort erreicht.

In Figur 2 ist ein Postgut 8, im Beispiel ein Briefumschlag, mit einer erfindungsgemäßen Frankierung und Adressierung gezeigt. Diese weist ein Adressfeld 81 für die Adressierung, ein optionales Absenderfeld 82 für die Absenderadresse, einen Gebührenstempel 83, einen Datenstempel 84 und ein Etikett 85 auf. Das Etikett 85 ist optional und dient quasi als Fingerabdruck für das Postgut, wozu auf dem Etikett enthaltene Etikettdaten in dem Datenstempel 84 in nicht manipulierbarer Form ebenfalls enthalten sind. Dadurch soll verhindert werden, dass der Gebührenstempel 83 und der Datenstempel 84 ausgeschnitten oder kopiert und auf ein weiteres Postgut geklebt und illegal wiederverwendet werden. Dazu müsste zusammen mit dem Datenstempel 84 auch das Etikett 85 wiederverwendet werden, das beispielsweise so gestaltet sein kann, dass es bei seiner Ablösung zerstört wird und/oder sich nicht

kopieren lässt, wie beispielsweise Hologramme, Wasserzeichen, Reliefdrucke u.s.w. Im übrigen kann der Datenstempel 84 so ausgestaltet sein, dass er maschinenlesbar ist, die Adresse des Adressaten enthalten ist und zur maschinellen Sortierung des Postgutes verwendet werden kann. In diesem Fall könnte die Frankierung also auch nur für ein an denselben Adressaten gerichtetes Postgut verwendet werden. Die Anordnung, Größe und Ausgestaltung der einzelnen Felder 81 bis 85 kann natürlich auch anders als gezeigt erfolgen.

In den Figuren 3 bis 6 sind zur Erläuterung einzelner Vorgänge Protokolle mit einzelnen Protokollschritten dargestellt. Zum Verständnis dieser Protokolle, die im wesentlichen auf der Schwierigkeit der Berechnung von diskreten Logarithmen beruhen, sollen zunächst einige der verwendeten Bezeichnungen und Definitionen erläutert werden. Die Bezeichnungsweise ist ähnlich der in der US 5,521,980 verwendeten Bezeichnungsweise, in der ein elektronisches Zahlungssystem beschrieben ist und auf die hinsichtlich weiterer Erläuterungen der Bezeichnungsweise und weiterer Definitionen hiermit ausdrücklich verwiesen sei.

Es sollen bezeichnen: Z die Menge der ganzen Zahlen, q eine Primzahl, G eine Familie endlicher, multiplikativer Abel'scher Gruppen G_q der Ordnung q. Weiter seien fuer eine gegebene Gruppe G_q Potenzen g^x mit ($g \in G_q$ und $x \in Z$) definiert durch wiederholte Multiplikation in G_q. Für einen gegebenen Generator g der Gruppe G_q und ein Element $z \in G_q$ heisst die kleinste nicht-negative ganze Zahl x, sofern sie $z = g^x$ erfüllt, diskreter Logarithmus von z bezüglich g. Seien allgemeiner l Generatoren $g_1,...,g_l \in G_q$ gegeben, dann heisst ein Tupel $(x_1,...,x_l)$, das $z = \prod_{i=1}^{l} g_i^{x_i}$ erfüllt, eine diskrete Repräsentation von z bezüglich $g_1,...,g_l$.

Im folgenden werden Familien von Gruppen G_q benutzt, die effiziente Algorithmen haben zum Multiplizieren von Gruppenelementen, gleichverteilt zufälligen Wählen von Gruppenelementen, und Testen zweier Gruppenelemente auf Gleichheit. Ausserdem sei das Berechnen diskreter Logarithmen schwer, d.h. nicht in polynomialer Zeit in der Bitlänge von q möglich. Obwohl bisher die letzte Eigenschaft für keine Familie von Gruppen bewiesen worden ist, gibt es Kandidaten, denen man diese Eigenschaften nach intensiver Erforschung über mehrere Jahrzehnte zuschreibt. Man nennt dies die diskrete Logarithmusannahme oder diskrete

Repräsentationsannahme. Beide sind äquivalent.

Ein Kandidat sind große zyklische Untergruppen der multiplikativen Gruppen Z_p^* endlicher Körper von Residuen modulo einer großen Primzahl p. Groß heisst hier dass p mindestens 1024 bit lang ist. Andere (allerdings weniger lang untersuchte) Kandidaten sind Familien bestimmter elliptischer Kurven, genauer große Untergruppen elliptischer Kurven. Die elliptischen Kurven sollten nicht super-singulär und von niedrigem Geschlecht sein. Konkrete Empfehlungen gibt es z.B. vom National Institute of Standards and Technology (NIST) [NIST99] (http://csrc.nist.gov/encryption). Gegenwärtiger Stand der Forschung ist, dass das Berechnen diskreter Logarithmen in den erstgenannten Kandidaten bei einer Modullänge von 1024 bit etwa so schwer ist wie das Berechnen diskreter Logarithmen in den letztgenannten Kandidaten bei einer Kurvenordnung von etwa 160 bit. Im folgenden wird die multiplikative Notation von G_q verwendet. Diese Notation kann leicht in die bei elliptischen Kurven übliche additive Notation übersetzt werden, indem Multiplikationen in G_q durch Addition und Potenzen in G_q durch skalare Vielfache von Punkten einer Kurve ersetzt werden.

Die in den Figuren 3 bis 6 gezeigten Protokolle sind in der für Algorithmen üblichen Schreibweise abgefasst: Durch eine Deklaration und eine Definition. Eine Protokolldeklaration, die jeweils in der ersten Zeile der Figur aufgeführt ist, besteht aus den formalen Ausgabeparametern, gefolgt von einem Zuweisungspfeil, gefolgt von dem Protokollnamen und den formalen Eingabeparametern in Klammern. Um die Lesbarkeit zu verbessern, sind alle Eingabe- und Ausgabeparameter eines Teilnehmers in eckigen Klammern eingeschlossen, wobei an die Klammer in Hochstellung die Abkürzung des Teilnehmers (S für Benutzer, P für Postgebühreneinrichtung) angefügt ist. Formale Eingabeparameter können von einem Protokollteilnehmer allein oder von allen Protokollteilnehmer gemeinsam genommen werden. Erstere heissen private Eingaben, letztere heissen gemeinsame Eingaben. Eine Protokolldefinition erfolgt in Matrixschreibweise, wobei die Handlungen jedes Teilnehmers in Spalten untereinander geschrieben sind und jede Spalte mit dem Teilnehmernamen überschrieben ist. Nacheinander folgende Handlungen eines Teilnehmers können zu Blöcken zusammengefasst werden.

Protokollhandlungen werden in der üblichen mathematischen Schreibweise mit einigen speziellen Symbolen geschrieben. Die gleichverteilt zufällige Wahl eines

Elements aus einer Menge A und die Zuweisung dieses Elementes an eine Variable a wird durch $a \in_R A$ bezeichnet. Die Auswertung eines Ausdrucks E und anschliessende Zuweisung des Ergebnisses an a wird mit $a \leftarrow E$ bezeichnet. H bezeichnet eine Pseudo-Zufalls-Hash-Funktion, die nach Eingabe einer beliebigen binären Zeichenfolge einen Wert aus Z_q zurückgibt. Es sei erlaubt eine H mit einer beliebigen Anzahl Argument zu schreiben. In diesem Fall sei der Input an H die Verkettung der binären Repräsentierungen aller Argumente. Arithmetische Operationen sind entweder in G_q, d.h. Multiplikation mod p, oder in Z_q, d.h. Addition und Multiplikation mod q, geschrieben. Im folgenden sind Multiplikation und Potentzierung G_q die häufigsten Operationen. Diese Operation wird ohne den Zusatz "mod p" geschrieben. Die Addition und Multiplikation in Z_q erhält jeweils den Zusatz "mod q", so dass in jedem Fall klar ist, welche Operation gemeint ist. Schickt ein Teilnehmer eines Protokolls den Wert seiner Variablen a an einen anderen Teilnehmer, so zeigt ein mit a bezeichneter Pfeil $\xrightarrow{a}$ von der Spalte des sendenden zur Spalte des empfangenden Teilnehmers (siehe Fig. 3 und 4). Aufrufe von Protokollen oder Algorithmen sind in der üblichen Schreibweise bezeichnet. Der Ausdruck "proceed iff P" mit P als Boolschem Prädikat bedeutet, dass die Protokollausführung nur dann weitergeht, falls und nur falls P gültig ist. Anderenfalls wird das Protokoll beendet und die Teilnehmer geben eine entsprechende Fehlermeldung aus.

In den folgenden Protokollen bezeichnen p eine große Primzahl, q einen großen Teiler von $p-1$ und G_q die eindeutige Untergruppe der multiplikativen Gruppe des Körpers Z_p, die die Ordnung q hat. Weiter seien g_1, g_2, G, G_0 vier Generatoren von G_q, die unabhängig voneinander und gleichverteilt zufällig beim Systemstart gewählt werden. Die Postgebühreneinrichtung P wählt einen privaten Schlüssel $x \in Z_q^*$ gleichverteilt zufällig und berechnet den korrespondierenden öffentlichen Schlüssel $y = g^x \bmod p$. Digitale Münzen (auch "piece of postage" (PoP)) sind Tupel (A, B, σ), wobei $A, B \in G_q$ und $\sigma = (z, a, b, r)$ eine digitale Signatur aus dem Bereich $G_0 \times G_0^2 \times G_0^2 \times Z_q$. Eine digitale Münze ist *gültig* bezüglich einem öffentlichen Schlüssel y, wenn sie folgende Gleichung erfüllt:

$$verifyPoP\left(y,A,B,\left(z,a,b,r\right)\right)\equiv\left(G^r=\left(ya_1\right)^c b_1\wedge m^r=\left(za_2\right)^c b_2\right) \qquad (1)$$
$$\text{mit } c=H\left(A,B,z,a,b\right)$$

Indizia bzw. Datenstempel sind in ihrer digitalen Form Tupel $\left(A,B,\left(z,a,b,r\right)s,rcpt,d/t\right)$, wobei der erste Teil $\left(A,B,\left(z,a,b,r\right)\right)$ eine digitale Münze ist, und der zweite Teil $\left(s,rcpt,d/t\right)$ die Leistung spezifizieren, die mit diesem Indizium bezahlt werden kann. Dabei sind $s\in Z_q^3$ ein Hilfswert, der die Deanonymisierung des Benutzers im Betrugsfall ermöglicht, *rcpt* der Empfänger und *d/t* das Erstelldatum und die Erstellzeit des Indiziums. Weitere Daten über die Herkunft des Indiziums können hinzugefügt werden. Ein Datenstempel ist gültig, wenn die folgende Gleichung erfüllt ist:

$$verifyInd\left(y,A,B,\left(z,a,b,r\right)s,rcpt,d/t\right)\equiv\left(AB\neq 1\wedge g_1^{s_1}g_2^{s_2}G_0^{s_3}=AB^c\right) \qquad (2)$$
$$\text{mit } c=H\left(A,B,z,a,b,r,rcpt,d/t\right)$$

In Figur 3 ist ein Teil des bei der Eröffnung eines Postgebührenkontos ablaufenden Protokolls gezeigt. Bevor ein Benutzer *S* ein Postgebührenkonto eröffnen kann, muss er gleichverteilt zufällig eine private digitale Identität $\left(u_1,u_2\right)\in Z_q^{*2}$ wählen und seine zugehörige öffentliche digitale Identität $I=g_1^{u_1}g_2^{u_2}\bmod p$. Anschließend identifiziert er sich gegenüber der Postgebühreneinrichtung *P*, zum Beispiel mittels eines Ausweises, und eröffnet sein elektronisches Postgebührenkonto. Als Kontonummer verwendet er seine öffentliche digitale Identität *I*. Als Nachweis, dass *I* seine rechtmäßige öffentliche Identität ist, beweist er, eine diskrete Repräsentation von *I* bezüglich der Generatoren g_1, g_2 (nämlich seine private digitale Identität $\left(u_1,u_2\right)$) zu kennen, ohne diese diskrete Repräsentation der Postgebühreneinrichtung zu zeigen. Dies geschieht in den Blöcken 41 bis 44 auf interaktive Weise zwischen dem Benutzer *S* und der Postgebühreneinrichtung *P*. Wenn die Postgebühreneinrichtung die Identifizierung akzeptiert und das Protokoll erfolgreich durchlaufen wird ($acc=True$), so wird im Namen des Benutzers *S* ein

neues Postgebührenkonto mit Nummer *I* eröffnet.

In Figur 4 ist ein Protokoll gezeigt, das zum Herunterladen von digitalen Münzen durchlaufen wird. Gemeinsame Eingabe ist die Kontonummer *I* und der öffentliche Schlüssel *y* der Postgebühreneinrichtung. Private Eingabe der Postgebühreneinrichtung *P* ist ihr privater Schlüssel *x*. Private Eingabe des Benutzers *S* ist seine private digitale Identität (u_1,u_2). Zunächst beweist der Benutzer, daß er eine diskrete Repräsentation von I besitzt (Block 51). Das Protokoll ist in Fig. 3 gezeigt. Die Postgebühreneinrichtung und der Benutzer nehmen die gemeinsame Eingabe I und der Benutzer nimmt als private Eingabe seine private digitale Identität (u_1,u_2). Nun wählt der Benutzer gleichverteilt zufällig zwei Werte $w_1, w_2 \in Z_q$ und berechnet $a \leftarrow g_1^{w_1} g_2^{w_2}$. Dieser Wert a wird an die Postgebühreneinrichtung geschickt, die daraufhin gleichverteilt zufällig einen Wert *c* wählt und ihn dem Benutzer schickt. Hierauf antwortet der Benutzer mit dem Wertepaar $(r_1,r_2) = (cu_1 + w_1 \bmod q, cu_2 + w_2 \bmod q)$. Falls das vom Benutzer zurückgegebene Wertepaar die Gleichung $g_1^{r_1} g_2^{r_2} = h^c a$ erfüllt, so akzeptiert die Postgebühreneinrichtung *I* als öffentliche digitale Identität des Benutzers und damit als Kontonummer. Als nächstes wählt der Benutzer gleichverteilt zufällig die Werte *u*, *v* gemäß Block 52. Gleichzeitig wählt die Postgebühreneinrichtung einen Wert *t* und berechnet anschließend die Komponenten *z*,*a*,*b* gemäß Block 53. Die Postgebühreneinrichtung schickt z, a, b an den Benutzer. Dieser wählt daraufhin gleichverteilt zufällig weitere Werte $\omega \in Z_q^*$ und $\alpha = (\alpha_1,\alpha_2,\alpha_3) \in Z_q^3$. Sodann berechnet er sukzessiv die Werte $I', z', A', B', a', b', c', c$ gemäß Block 54. Als nächstes schickt er den Wert *c* an den die Postgebühreneinrichtung, die mit einem Wert *r* gemäß Block 55 antwortet. Schliesslich berechnet der Benutzer den Wert *r'* und akzeptiert die erhaltene digitale Münze $(A', B', (z', a', b', r'))$, wenn sie gültig ist (siehe Gleichung (1) oben) bezüglich dem öffentlichen Schlüssel *y* der Postgebühreneinrichtung (siehe Block 56). Außerdem speichert sich der Benutzer die diskreten Repräsentationen α, β von *A* und *B* für die erhaltene digitalen Münze.

Wenn der Benutzer ein Postgut frankieren will, wählt er eine geeignete digitale Münze $(A, B, (z, a, b, r))$ aus und berechnet das entsprechende Indizium. In diese

Berechnung gehen der Empfänger *rcpt* des Postguts, das Datum und die Zeit der Erstellung *d/t* des Indiziums und ggf. weitere relevante Daten ein. Zusätzlich zur Postgebühreneinheit muss der Benutzer auch die entsprechenden diskreten Repräsentationen α, β von *A* bzw. *B* eingeben. Figur 5 zeigt die Berechnungen, die der Benutzer durchführt (Block 61).

Wenn ein so frankiertes Postgut zur Prüfeinrichtung gelangt, kann das Indizium gemäß der obigen Gleichung (2) verifiziert werden. Es liegt im Ermessen der Prüfeinrichtung welche Quote durchlaufender Postgüter überprüft wird. Wenn ein Benutzer eine erhaltene digitale Münze dazu benutzt, mehr als ein Indizium und damit mehr als eine Frankierung zu erzeugen, obwohl die digitale Münze nur zur Frankierung eines einzigen Stückes Postgut ausgestaltet ist, dann kann die Prüfeinrichtung diese doppelte Benutzung daran erkennen, daß die Komponenten A,B in einem früher geprüften Indizium benutzt worden sind. In diesem Fall seien die beiden Indizia mit c_1, c_2 bezeichnet und die entsprechenden *s*-Komponenten als $s_1 = (s_{11}, s_{12}, s_{13})$ und $s_2 = (s_{21}, s_{22}, s_{23})$. Nun kann die Prüfeinrichtung die private digitale Identität (u_1, u_2) des betrügerischen Benutzers mit den in Block 71 der Figur 6 gezeigten Rechenschritten ermitteln und daraus die Kontonummer $I = g_1^{u_1} g_2^{u_2} \bmod p$ des betrügerischen Benutzers.

Bei dem erfindungsgemäßen Frankierverfahren und dem erfindungsgemäßen Frankiersystem ist keine zusätzliche Hardware für eine Sicherheitseinrichtung zur Sicherung und Abrechnung von Postgebühren erforderlich, sondern die Realisierung ist mittels eines herkömmlichen Computers und Druckers möglich. Dadurch kann ein solches System deutlich kostengünstiger realisiert werden, weshalb die Anwendung auch für einen größeren Massenmarkt interessant ist. Gleichzeitig werden aber hohe Sicherheitsanforderungen erfüllt. Es ist weiter möglich, die wesentlichen Verfahrensschritte durch reine Software zu realisieren, die mit einfachen Mitteln ausgetauscht und verbessert werden kann. Es ist auch nicht erforderlich, dass jeder Benutzer sein individuelles Schlüsselpaar z.B. für ein digitales Signatursystem besitzt. Die Benutzer und die Prüfeinrichtung müssen lediglich den öffentlichen Schlüssel des Postdienstes bzw. der Postgebühreneinrichtung kennen. Dieser kann beispielsweise auf einer Internetseite des Postdienstes veröffentlicht sein und die zugehörigen öffentlichen Zertifikate können in einen Standard-Webbrowser integriert sein. Im Gegensatz dazu besitzt bei den bekannten Lösungen jeder Benutzer seinen eigenen individuellen Unterschriftenschlüssel, was im Gegenzug erfordert, dass der Postdienst

entweder die entsprechenden Verifizierungsschlüssel verwalten und speichern muss oder dass jeder Datenstempel den entsprechenden Verifizierungsschlüssel und das Verifizierungszertifikat enthalten muss. Wenn es bei den bekannten Lösungen einem Betrüger gelingt, den Unterschriftenschlüssel einer Sicherheitseinrichtung eines Benutzers zu brechen, kann er ohne Risiko der Entdeckung in beliebiger Weise Frankierungen erzeugen. Im Gegensatz zu diesem Hardwareschutz bei den bekannten Lösungen, die den Aufbruch der Sicherheitseinrichtung verhindern sollen, wird bei der erfindungsgemäßen Lösung ein Schutz mit kryptografischen Mitteln gewährleistet. Außerdem lassen sich bei der erfindungsgemäßen Lösung weitere Sicherheitsanforderungen und Ansprüche an den Bedienkomfort einfacher und kostengünstiger realisieren.

Figur 7 zeigt einen Testabdruck eines Datenstempels mit einer Datenmatrix von 40 x 40 Elementen, also der kleinsten Datenmenge, der in Tabelle 1 genannten Optionen. Der abgedruckte Datenstempel ist maschinenlesbar und enthält die elektronische Münze, deren Wert sowie deren Verfallsdatum wie auch weitere Angaben, die die Frankierung individualisieren. Die Datenmatrix 100 kann selbstverständlich auch aus einer anderen Elementenzahl von mx x n Elementen gebildet werden. Links neben der bedruckten Datenmatrix 100 ist ein üblicher Werbeaufdruck wiedergegeben.

Vorstehend wurde ein Verfahren zum maschinellen Frankieren von Postgut und zur Überprüfung der Frankierung beschrieben. Das erfindungsgemäße Konzept lässt sich jedoch überall im elektronischen Handel (e-commerce, IE-cash-Systeme) einsetzen, beispielsweise ist es ohne weiteres möglich, dass mittels der Erfindung in dezentralen und offenen Systemen auch Dienstleistungen wie beispielsweise die Ausgabe von Karten und Tickets (Theaterkarten, Fahrkarten etc.) abgewickelt werden. Wird beispielsweise eine Fahrkarte von dem Fahrkartennutzer selbst erzeugt, so enthält der Fahrkartenabdruck alle Daten der Fahrkarten-individuellen elektronischen Münze. Da jede Fahrkarte individualisiert ist, ist eine mehrfache Verwendung der Fahrkarte ausgeschlossen.

Ansprüche

1. Verfahren zum maschinellen Frankieren von Postgut (8) und zur Prüfung der Frankierung, wobei Postgebühren in elektronischer Form als elektronische Münzen gespeichert und abgerechnet werden und wobei auf das Postgut (8) ein maschinenlesbarer, die elektronische Münze enthaltener Datenstempel aufgebracht wird, wobei für jedes Stück Postgut eine individuelle, von denen für andere Stücke Postgut erzeugten elektronischen Münzen unterscheidbare elektronische Münze erzeugt wird und anhand des die elektronische Münze enthaltenen Datenstempels (84) eine Prüfung auf mehrfache Verwendung von elektronischen Münzen und/oder Datenstempeln erfolgt.

2. Verfahren nach Anspruch 1,
dadurch gekennzeichnet, dass die Prüfung durch Vergleich der zu prüfenden elektronischen Münze (84) mit einer in einer Datenbank (14) gespeicherten benutzten elektronischen Münze erfolgt.

3. Verfahren nach Anspruch 1 oder 2,
dadurch gekennzeichnet, dass jeder Datenstempel (8) bzw. die in ihr enthaltene elektronische Münze ein (individuelles) Verfallsdatum enthält.

4. Verfahren nach Anspruch 3,
dadurch gekennzeichnet, dass in der Datenbank (14) nur die bis zu einem maximalen Verfallsdatum gültigen, bereits benutzten elektronischen Münzen gespeichert werden.

5. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass die Postgebühren, die eine elektronische Münze repräsentieren, als Postgebühreneinheiten gespeichert werden, wobei jede Postgebühreneinheit eine postgutindividuelle Codierung aufweist und dass die Codierung derart bei der Erzeugung der elektronischen Münze für ein Postgut (8) verwendet wird, das anhand des Datenstempels (84) überprüfbar ist, ob eine Postgebühreneinheit bzw. elektronische Münze bereits zur Frankierung eines Postguts verwendet worden ist.

6. Verfahren nach Anspruch 5,
dadurch gekennzeichnet, dass mehrere Postgebühreneinheiten zur Frankierung eines

Postguts (8) kombinierbar sind und/oder eine Postgebühreneinheit aus mehreren elektronischen Münzen bestehen kann.

7. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass die elektronische Münze nur ganz bestimmte Daten authentisiert.

8. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass die Postgebühreneinheiten in mehreren Untereinheiten unterteilt sind und dass die Untereinheiten zur Frankierung unterschiedlicher Stücke Postgut verwendbar sind.

9. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass die Erzeugung der Postgebühreneinheiten bei deren Erwerb von einer Postgebühreneinrichtung mittels eines nur ihrbekannten (geheimen) Schlüssels erfolgt.

10. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass in dem Datenstempel (84) bzw. in der generierten elektronischen Münze dessen bzw. deren Erstelldatum und Erstellzeit, die frankierte Postgebühr und/oder der Adressat des Postguts (8) (in nicht manipulierbarer) Form enthalten sind.

11. Verfahren nach einem der vorhergehenden Ansprüche,
dadurch gekennzeichnet, dass in dem Datenstempel (84) bzw. der generierten elektronischen Münze das Postgut (8) charakterisierende Postgutdaten, insbesondere physikalische Eigenschaften des Postguts charakterisierende Postgutdaten, enthalten sind.

12. Verfahren nach Anspruch 11,
dadurch gekennzeichnet, dass als Postgutdaten die Art und/oder Oberflächenstruktur des Verpackungsmateriales des Postguts einmalig charakterisierende und/oder auf einem zusätzlich auf dem Postgut aufgebrachten Etikett (85) befindliche Etikettdaten verwendet werden.

13. Verfahren zum maschinellen Frankieren von Postgut (8),
wobei Postgebühren als elektronische Münze in elektronischer Form gespeichert und

abgerechnet werden und wobei auf das Postgut (8) ein maschinenlesbarer die elektronische Münze enthaltener Datenstempel (84) aufgebracht wird, wobei für das Stück Postgut (8) ein individueller, von den für andere Stücke Postgut erzeugte elektronische Münze unterscheidbare elektronische Münze (84) erzeugt und auf das Postgut (8) aufgebracht wird, und zwar in der Art, dass anhand des die elektronische Münze enthaltenen Datenstempels (84) eine Prüfung auf mehrfache Verwendung von elektronischen Münzen und/oder Datenstempeln möglich ist.

14. System zur Durchführung des Verfahrens nach Anspruch 1,
- mit eine Frankiermaschine (2) zum maschinellen Frankieren von Postgut (8), umfassend eine Druckeinheit (22) zum Aufbringen eines maschinenlesbaren, unter Umständen verschlüsselten, Datenstempels (84) auf das Postgut (8) und eine Zentraleinheit (21) mit einem Gebührenmodul (23) zum Laden, Speichern und Abrechnen von Postgebühren, mit einem Drucksteuermodul (25) zum Steuern der Druckeinheit (22), und
- mit einer Postgebühreneinrichtung (11) zum Ausgeben von Postgebühreneinheiten und
- mit einer Prüfeinrichtung (13) zum Prüfen des Datenstempels, wobei ein kryptographisches Modul zum Verschlüsseln von Daten für den Datenstempel vorgesehen ist, welches derart ausgestaltet ist, dass für jedes Stück Postgut (8) ein individueller, von den für andere Stücke Postgut unterscheidbarer Datenstempel (84) erzeugt wird, und dass die Prüfeinrichtung ausgestaltet ist zur Überprüfung auf mehrfache Verwendung von Postgebühren und/oder Datenstempeln anhand des Datenstempels (84).

15. System nach Anspruch 14,
dadurch gekennzeichnet, dass der Datenstempel (84) die Informationen einer elektronischen Münze enthält und die elektronische Münze für jede Frankierung individualisiert ist, so dass sich die elektronischen Münzen jeder Frankierung voneinander auch dann unterscheiden, wenn der gleiche Gebührenwert auf das Postgut aufgedruckt ist.

16. System nach Anspruch 14 oder 15,
dadurch gekennzeichnet, dass die Prüfeinrichtung (13) eine Speichereinrichtung (14) aufweist zum Speichern benutzter Datenstempel bzw. benutzter elektronischer Münzen.

17. System nach Anspruch 16,
dadurch gekennzeichnet, dass die Postgebühreneinrichtung (11) eine Verschlüsselungseinrichtung (12) (Kryptografieeinrichtung) zum Verschlüsseln (Kryptografieren) von Postgebühreneinheiten aufweist.

18. Frankiermaschine (2) zum maschinellen Frankieren von Postgut (8), umfassend eine Druckeinheit (22) zum Aufbringen eines maschinenlesbaren, eine elektronische Münze enthaltenen Datenstempels auf das Postgut (8) eine Zentraleinheit (21) mit einem Gebührenmodul (23) zum Laden, Speichern und Abrechnen von Postgebühren, mit einem Drucksteuermodul (25) zum Steuern der Druckeinheit (22), wobei auf jedes Stück Postgut (8) ein individueller, von den für andere Stücke Postgut erzeugte Datenstempel unterscheidbarer Datenstempel (84) derart erzeugt wird, dass anhand des Datenstempels (84) eine Überprüfung auf mehrfache Verwendung von Postgebühren und/oder Datenstempeln und/oder elektronischer Münzen möglich ist.

19. Frankiermaschine nach Anspruch 18, dadurch gekennzeichnet, dass die Frankiermaschine im Wesentlichen durch einen konventionellen Computer mit einem konventionellen Drucker realisiert ist.

Zusammenfassung

Die Erfindung betrifft ein Verfahren zum maschinellen Frankieren von Postgut (8) und zur Prüfung der Frankierung, wobei Postgebühren in elektronischer Form gespeichert und abgerechnet werden und wobei auf das Postgut (8) ein Gebührenstempel (83) und ein maschinenlesbarer verschlüsselte Daten enthaltender Datenstempel (84) aufgebracht werden. Um ein solches Verfahren kostengünstiger auszugestalten, wobei gleichzeitig hohe Sicherheitsanforderungen erfüllt sein und eine Realisierung auf einem herkömmlichen Computer mit einem Drucker ohne weitere zusätzliche Hardware möglich sein sollen, wird erfindungsgemäß vorgeschlagen, dass für jedes Stück Postgut (8) ein individueller, von den für andere Stücke Postgut erzeugte Datenstempel unterscheidbarer Datenstempel (84) erzeugt und auf das Stück Postgut (8) aufgebracht wird und dass anhand des Datenstempels (84) eine Prüfung auf mehrfache Verwendung von Postgebühren und/oder Datenstempeln erfolgt. Bevorzugt wird diese Prüfung durch Vergleich eines zu prüfenden Datenstempels (84) mit vorher benutzten in einer Datenbank gespeicherten Datenstempel realisiert. Damit lassen sich insbesondere Betrüger ermitteln, die ohne Bezahlung Frankierungen erzeugen oder Frankierungen beispielsweise durch Kopieren mehrfach verwenden wollen. Die Erfindung betrifft außerdem ein System zur Durchführung eines solchen Verfahrens sowie eine entsprechend ausgestaltete Frankiermaschine.

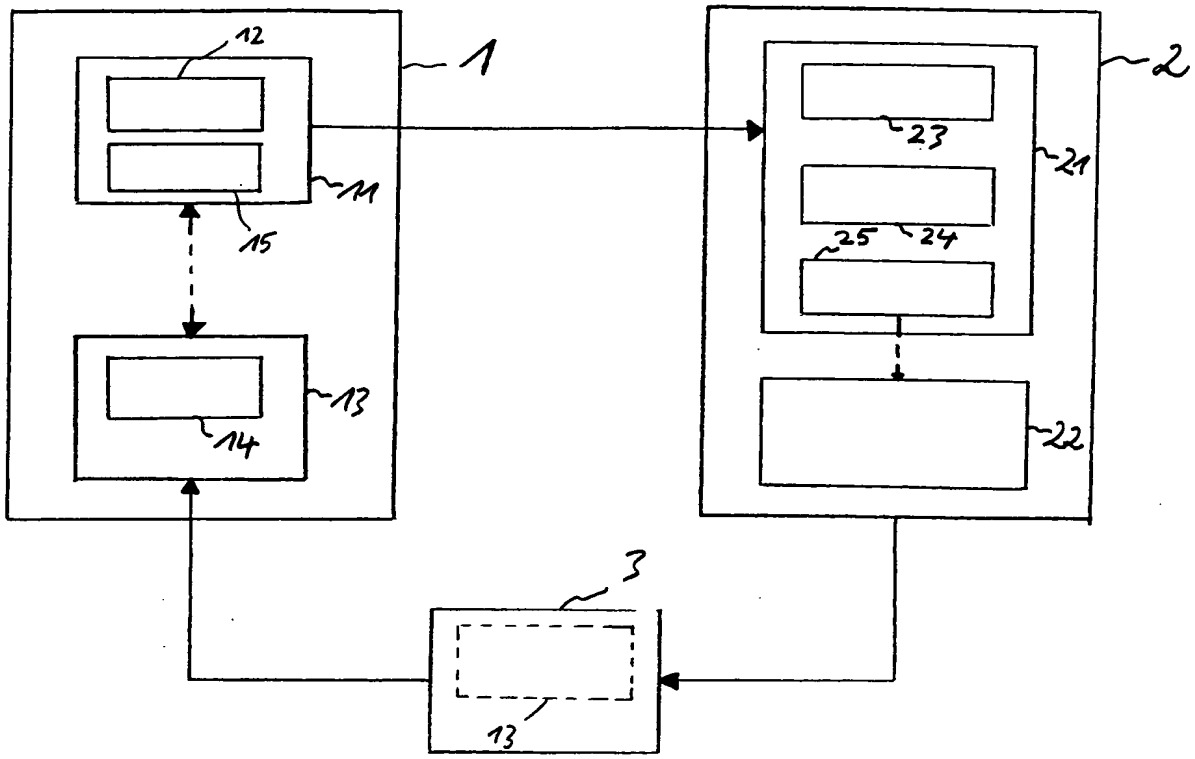

Fig. 1

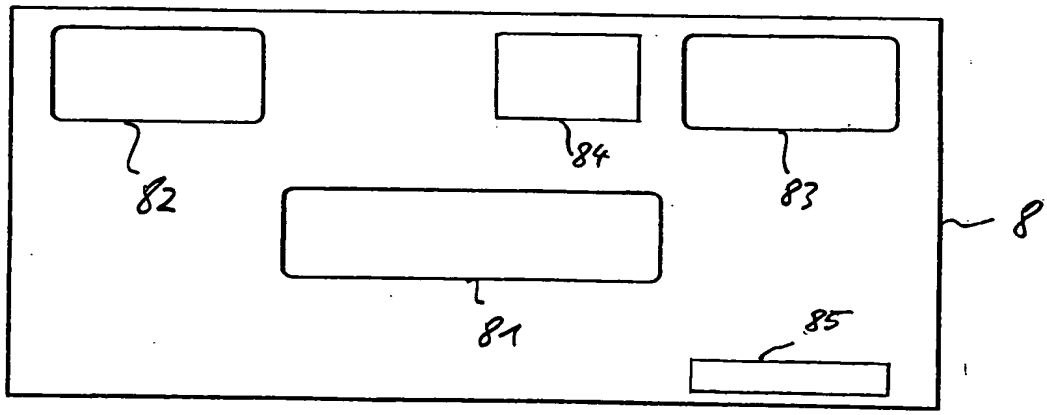

Fig. 2

$([acc]^P) \leftarrow prove([u_1, u_2, I]^S, [I]^P)$

user (S) — postal server (P)

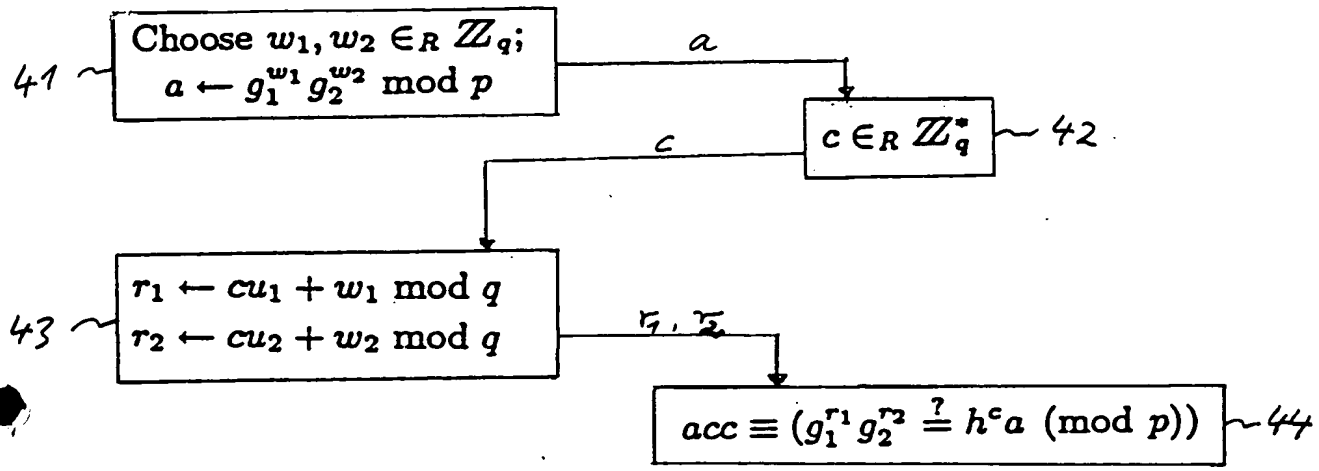

Fig. 3

$(s) \leftarrow indicium(A, B, \alpha, \beta, (z, a, b, r), rcpt, d/t)$

user

$$c \leftarrow \mathcal{H}(A, B, z, a, b, r, rcpt, d/t)$$
$$s = (s_1, s_2, s_3), \text{ where } s_i \leftarrow \alpha_i + c\beta_i \text{ for } i = 1, 2, 3$$

61

Fig. 5

$(u_1, u_2) \leftarrow identifyDS(c_1, s_1, c_2, s_2)$

mail check

$$u_1 \leftarrow \frac{s_{11}(c_2-1)+s_{21}(1-c_1)}{s_{13}(c_2-1)+s_{23}(1-c_1)} \bmod q$$
$$u_2 \leftarrow \frac{s_{12}(c_2-1)+s_{22}(1-c_1)}{s_{13}(c_2-1)+s_{23}(1-c_1)} \bmod q$$

71

Fig. 6

$([A', B', \alpha, \beta, \sigma']^S) \leftarrow download([u_1, u_2, y, I], [x, I]^P)$

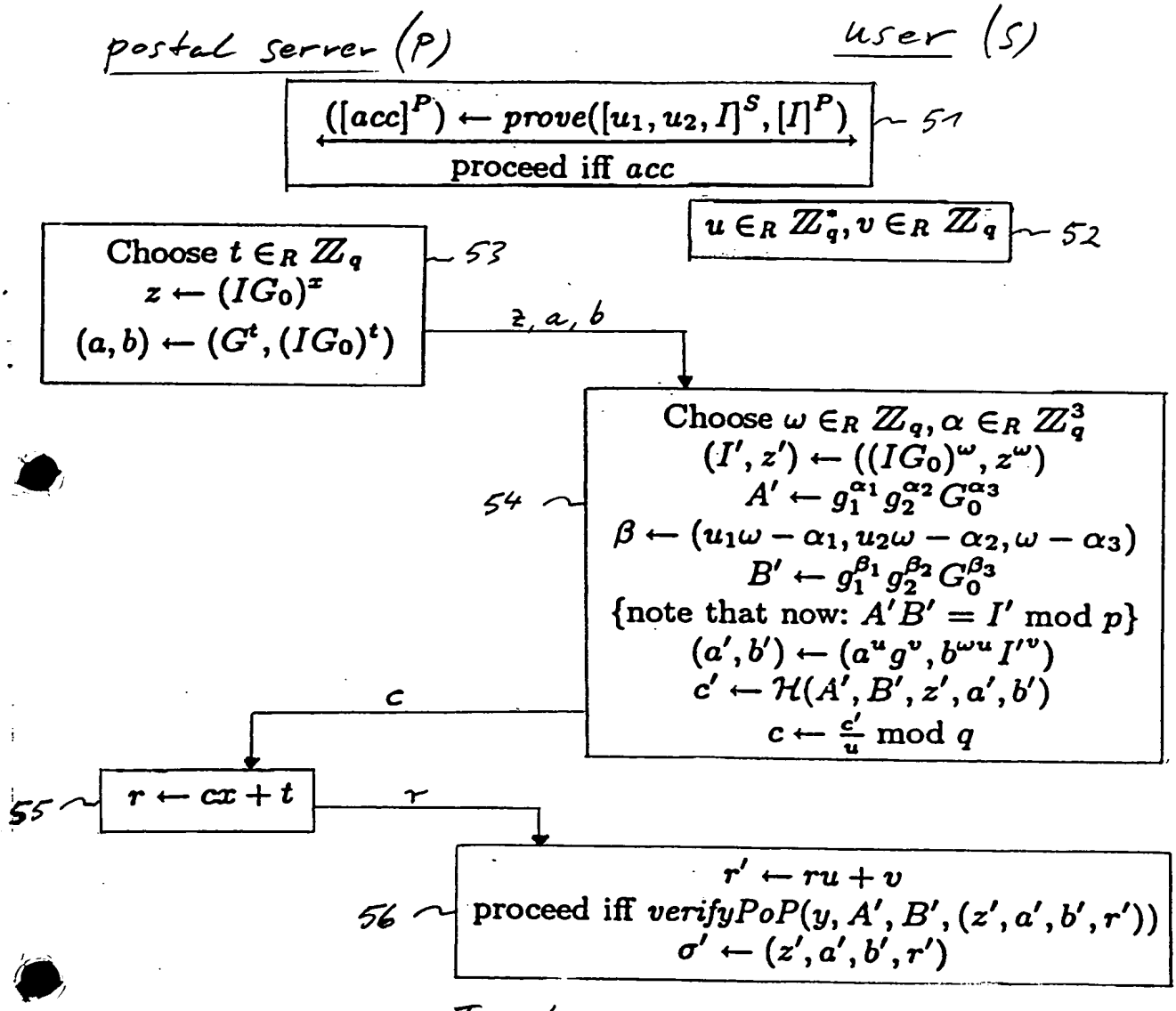

Fig. 4

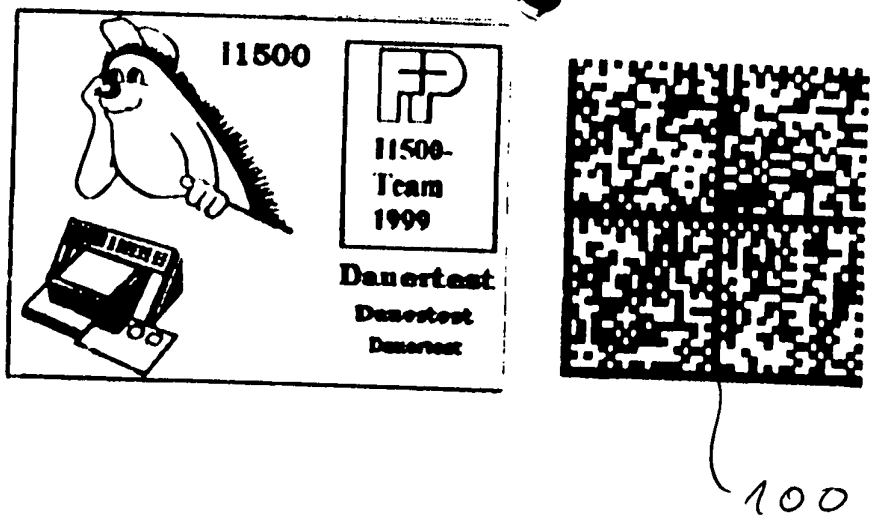

Fig. 7